12-14-2020

Text analytics-based framework for cyber-risk management

Kalpit Sharma
Indian Institute of Management Lucknow, fpm18012@iiml.ac.in

Arunabha Mukhopadhyay
Indian Institute of Management Lucknow, arunabha@iiml.ac.in

TREO
Technology, Research, Education, Opinion

Text analytics-based framework for cyber-risk management

Kalpit Sharma (kalpit@iiml.ac.in); Arunabha Mukhopadhyay (arunabha@iiml.ac.in)

Cyber-risk management has been at the helm of cybersecurity research since the advent of Newer Information Technology for businesses (Gordon et al. 2003). Cyber-risk management consists of three crucial steps, namely, cyber-risk assessment, cyber-risk quantification, cyber-risk mitigation. Cyber risk assessment methods intend to identify risky information assets (such as hardware and software systems, networks, customer data, and intellectual property), which can be attacked by cyber-attackers. (O'Reilly et al. 2018; Smith and Eloff 2002). It also identifies vulnerable paths in the communication networks, which can be exploited by cyber-attackers to launch various attacks.

Cyber-risk quantification follows a cyber-risk assessment and estimates the probability of identified risk with diverse methods to attach a monetary value to it. Cyber risk quantification methods rely on the probability of a risky incident occurring and a rigorous estimation of such events' loss amounts. Thus, the accuracy of such methods relies on thorough risk quantification as well as loss calculation. Therefore, the expected loss for an entity resulting from cyberattacks depends not only on the incident but also on our ability to accurately estimate its loss. These estimations also vary in their methodological rigor depending upon the type and granularity of data available to calculate them. Cyber risk quantification methods range from mathematical risk modeling to data mining methods using empirical data from security providers (Campbell and Stamp 2004).

On the other hand, cyber-risk mitigation focuses on elucidating ways to reduce risk and severity arising due to the compromise of risky assets by cyber-attackers. It considers subjective preferences and the decision-maker's risk appetite to suggest interventions (financial and technological) to mitigate risk (Kahneman and Tversky 1979; Kunreuther 1997).

In the proposed study, we aim to analyze textual data from the different stakeholders of the decision-making process to gauge the firms' cyber-risk. We will examine three research questions in this regard: (a) How can the text be used to quantify cyber-risk? (b) How to estimate a firm's loss through text data? (c) What are the ways to mitigate this cyber-risk? We intend to use data from cybersecurity news articles, tweets from cybersecurity experts, whitehat hackers, and cyber-threat intelligence reports to build a framework to investigate the questions mentioned earlier. The study will use sentiment analysis, topic modeling, and word vectors to categorize and group the articles according to cyber-risk scores and predict a cumulative score for the firm facing the cyber-attack. The second part of the study tries to estimate the firm's real impact by analyzing the engagement received on text data across platforms. The last stage of the framework generates strategies to mitigate the cyber-risk by visualizing the risk and severity of cyber-attack on the 2x2 heat matrix and helping the firms' management accept, reduce, or pass the cyber-risk.